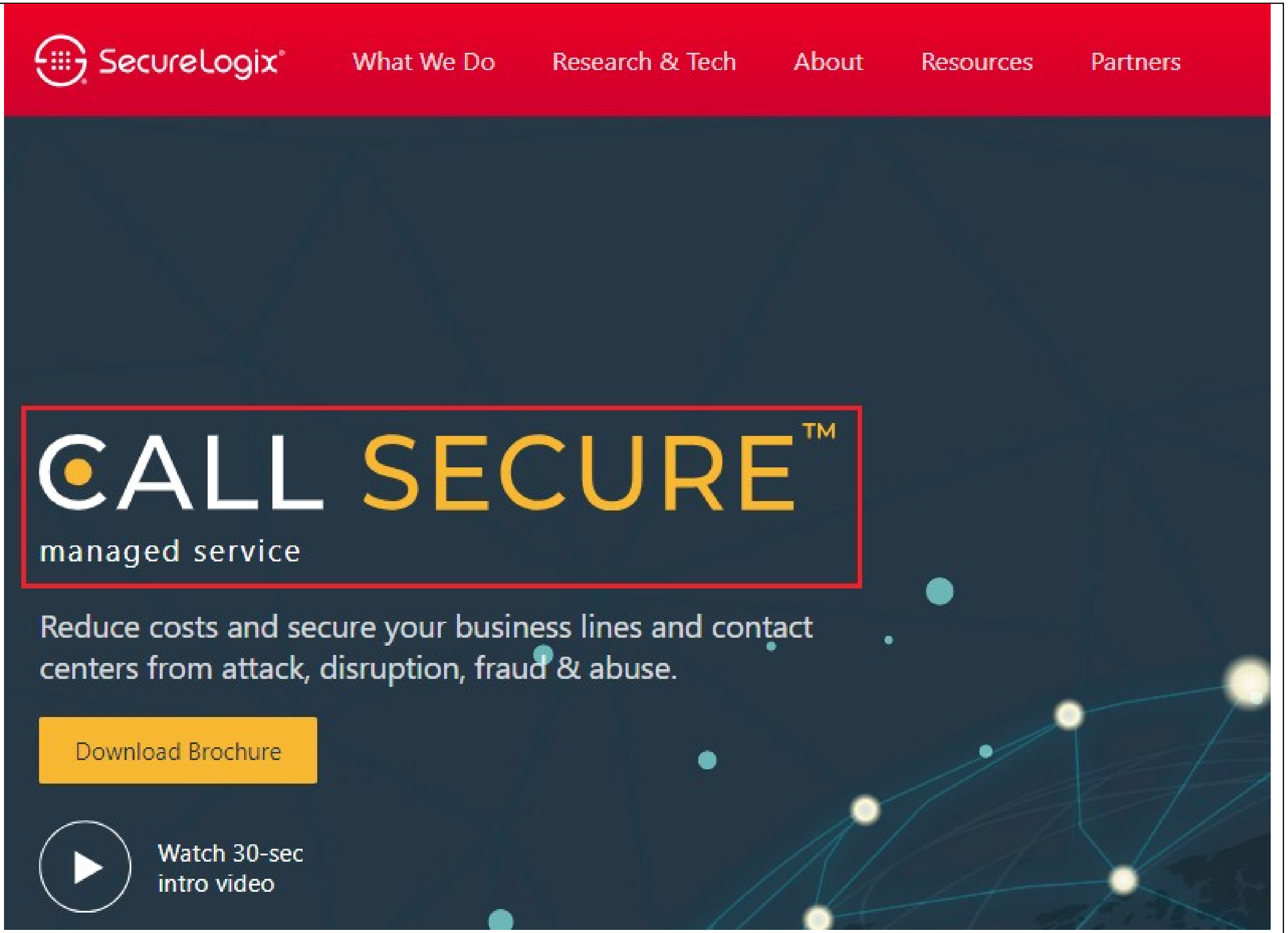
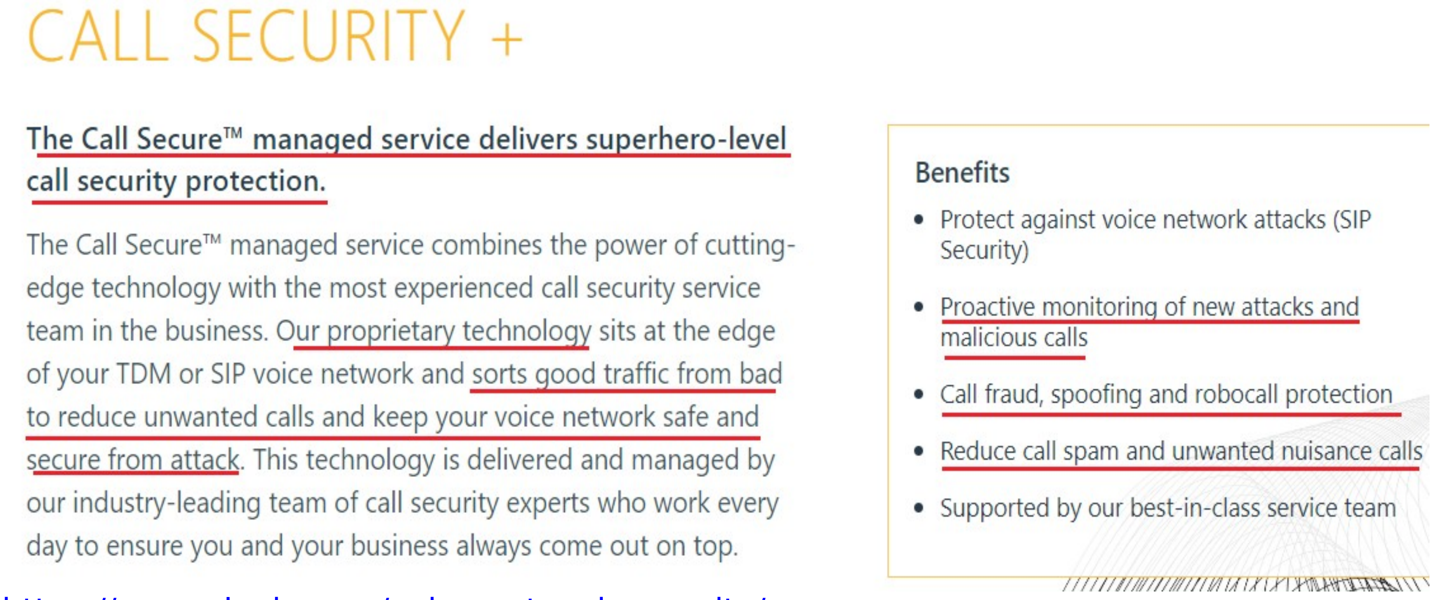
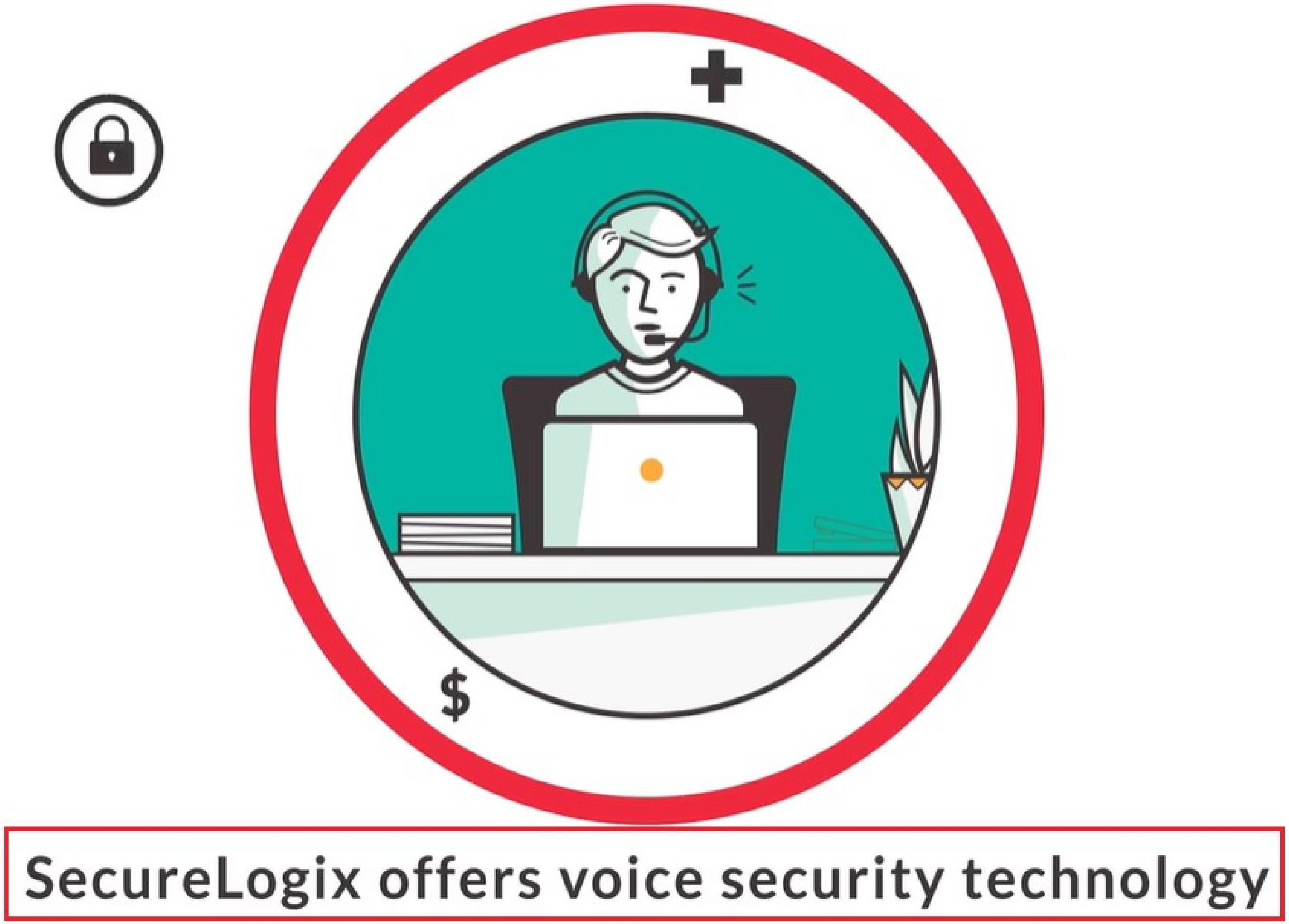
Exhibit 5

Charted claim:
Method claim:1

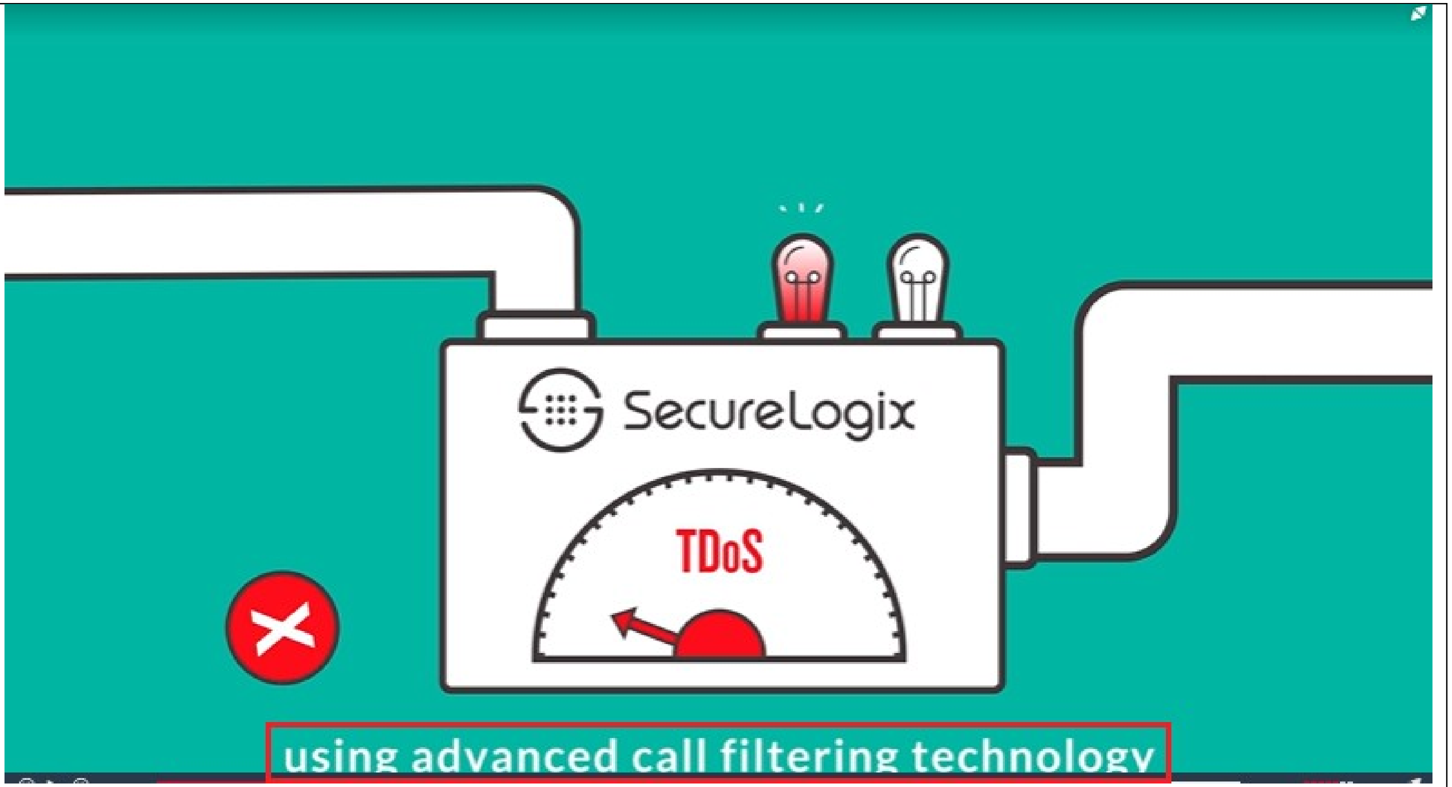
US9491286B2	SecureLogix - Call Secure™ managed service (“The accused instrumentality”)
1. A method comprising: receiving an incoming call from a caller at a call control unit communicatively coupled to, or resident within a telephone, the call control unit being positioned between a telecommunication service provider providing the incoming call and the telephone, the incoming call being associated with a telephone number and the caller; and	The accused instrumentality discloses a method (e.g., call security protection method) comprising receiving an incoming call (e.g., receiving an unwanted incoming call from the caller) from a caller (e.g., spam caller, robocaller, etc.) at a call control unit (e.g., Robocall/spam call protection unit of the Call Secure™) communicatively coupled to, or resident within a telephone (e.g., present within the smartphone using Call Secure™ managed service), the call control unit (e.g., Robocall/spam call protection unit of the Call Secure™) being positioned between a telecommunication service provider (e.g., calling service provider) providing the incoming call and the telephone (e.g., called user smartphone), the incoming call (e.g., unwanted incoming call) being associated with a telephone number (e.g., caller phone number) and the caller (e.g., the incoming call includes caller name, ID, phone number, etc.). As shown, Call Secure app includes call control feature for preventing calls from robocallers, spammers, etc. When a caller dials the number to a called user phone, the incoming call is received at the Robocall/spam call blocking unit of the Call Secure app installed within the caller user smartphone. The accused instrumentality identifies robocallers, spammers, etc., using the caller information such as caller name, phone number, etc.

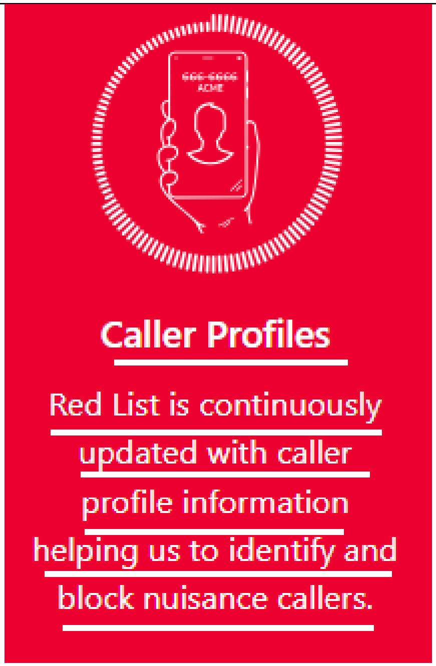
	 SecureLogix® What We Do Research & Tech About Resources Partners CALL SECURE™ managed service Reduce costs and secure your business lines and contact centers from attack, disruption, fraud & abuse. Download Brochure Watch 30-sec intro video https://securelogix.com/voice-network-security/

	 CALL SECURITY + **The Call Secure™ managed service delivers superhero-level call security protection.** The Call Secure™ managed service combines the power of cutting-edge technology with the most experienced call security service team in the business. Our proprietary technology sits at the edge of your TDM or SIP voice network and sorts good traffic from bad to reduce unwanted calls and keep your voice network safe and secure from attack. This technology is delivered and managed by our industry-leading team of call security experts who work every day to ensure you and your business always come out on top. **Benefits** • Protect against voice network attacks (SIP Security) • Proactive monitoring of new attacks and malicious calls • Call fraud, spoofing and robocall protection • Reduce call spam and unwanted nuisance calls • Supported by our best-in-class service team https://securelogix.com/voice-network-security/

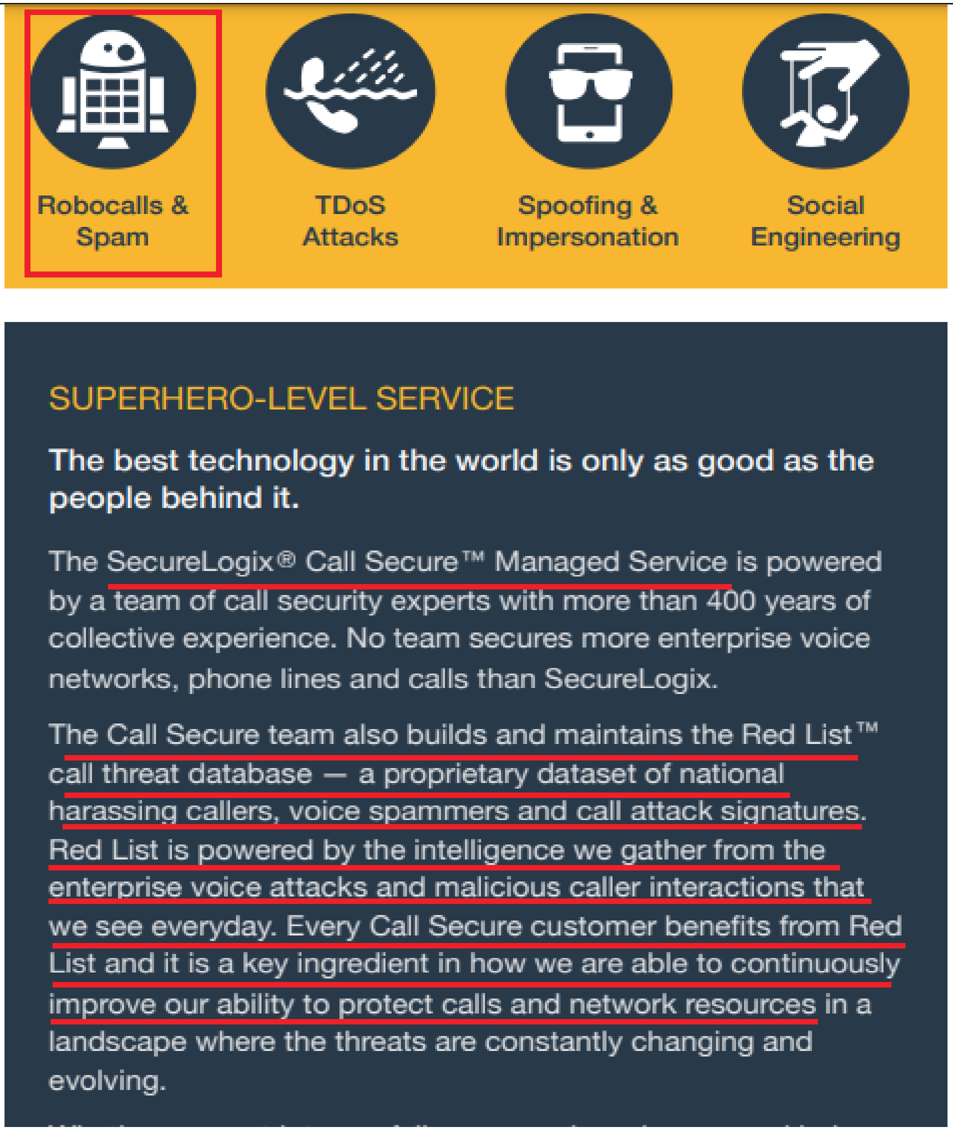
	 SecureLogix offers voice security technology https://securelogix.com/voice-network-security/

	   https://securelogix.com/voice-network-security/

	 using advanced call filtering technology https://securelogix.com/voice-network-security/

	 Caller Profiles Red List is continuously updated with caller profile information helping us to identify and block nuisance callers. https://securelogix.com/voice-network-security/
querying, by the call control unit, a server to determine whether additional information associated with the telephone number and the caller exists, and if so, determining whether the additional information indicates that a negative characteristic is	The accused instrumentality discloses querying, by the call control unit (e.g., Robocall/spam call protection unit of the Call Secure™), a server (e.g., server of the accused instrumentality) to determine whether additional information (e.g., additional information such as red list database, etc.) associated with the telephone number (e.g., caller phone number) and the caller exists (e.g., determine whether caller number is present in red list database), and if so, determining whether the additional information indicates that a negative characteristic (e.g., caller number present in red list database indicates a spam or robocall) is associated with at least one of the caller and the telephone number (e.g., caller phone number) and, if so, performing a first operation (e.g., blocking the call or not forwarding the call) on the incoming call responsively to the additional information (e.g., caller number is present in red list database), otherwise, performing a second operation (e.g., routing the call using call screening

associated with at least one of the caller and the telephone number and, if so, performing a first operation on the incoming call responsively to the additional information, otherwise, performing a second operation on the incoming call responsively to an absence of the additional information.	process) on the incoming call responsively to an absence of the additional information (e.g., caller number is absent in red list database). As shown, when the caller dials the number, the Robocall/spam call protection unit of the Call Secure™ queries the app server to determine whether the caller phone number is present in red list database, where the red list database is prebuilt caller profile database stored at server including harassing callers profiles to identify and block spam/ robocalls. If the server determines that the caller number is present in red list database which represent negative characteristic of the caller, the Robocall/spam call protection unit blocks the call and the call is not forwarded (e.g., a first operation). If the server determines that the caller number is absent in the red list database, the Robocall/spam call protection unit routes the call to the called user based on call screening process (e.g., a second operation) including solving puzzles, etc.



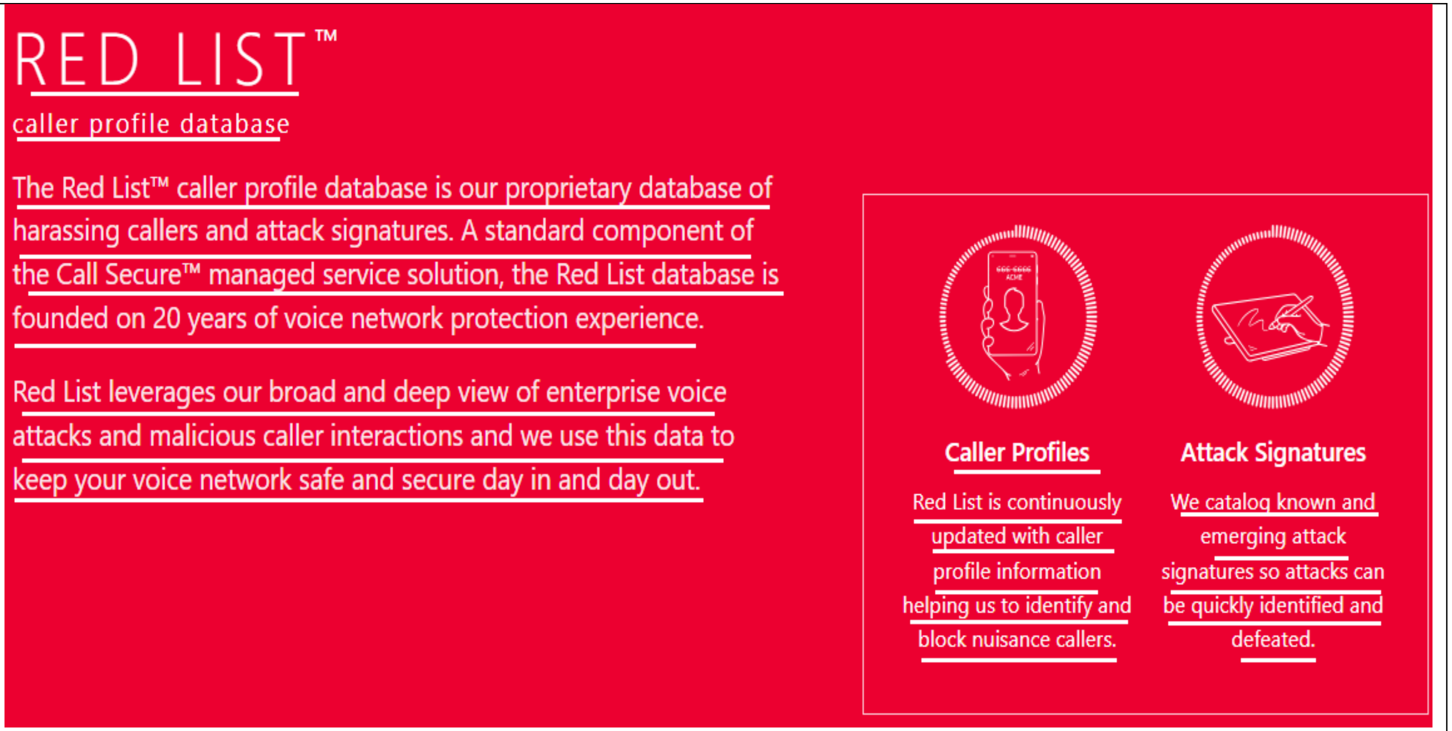
SUPERHERO-LEVEL SERVICE

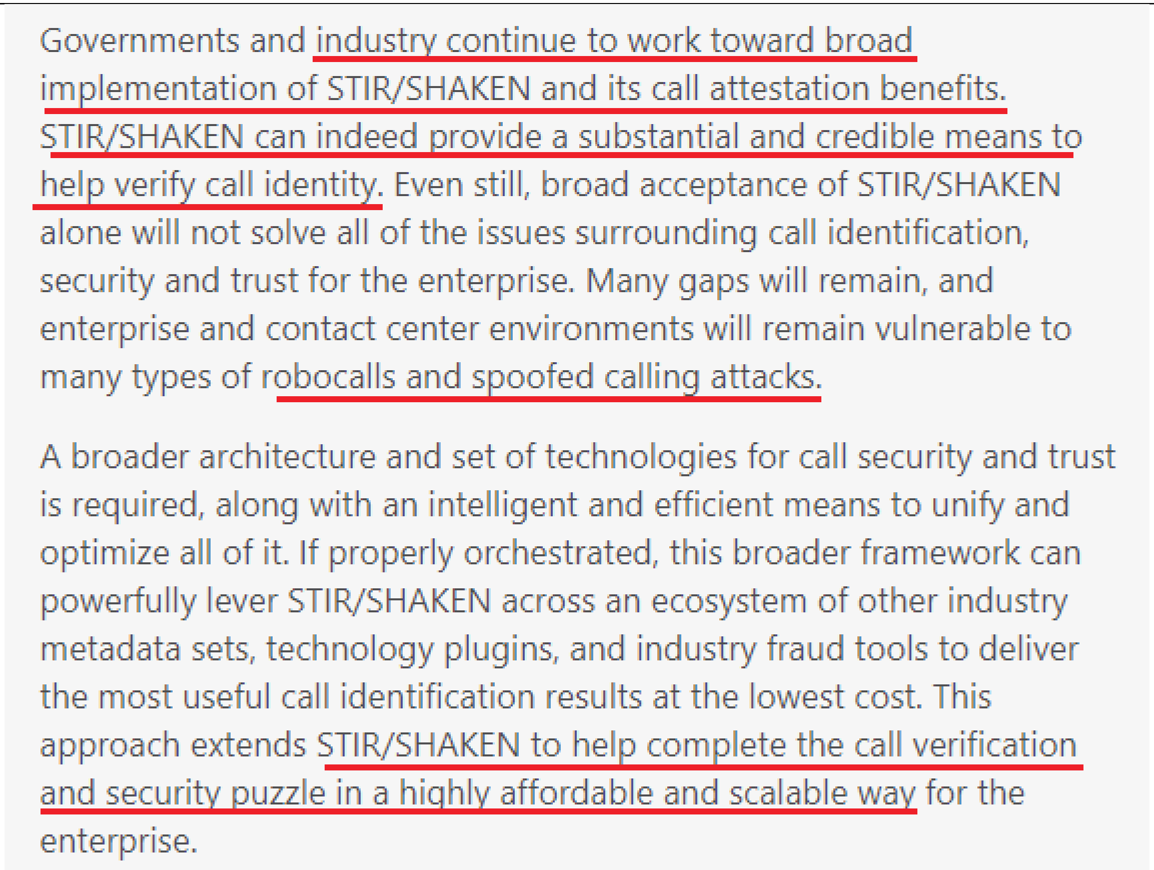
The best technology in the world is only as good as the people behind it.

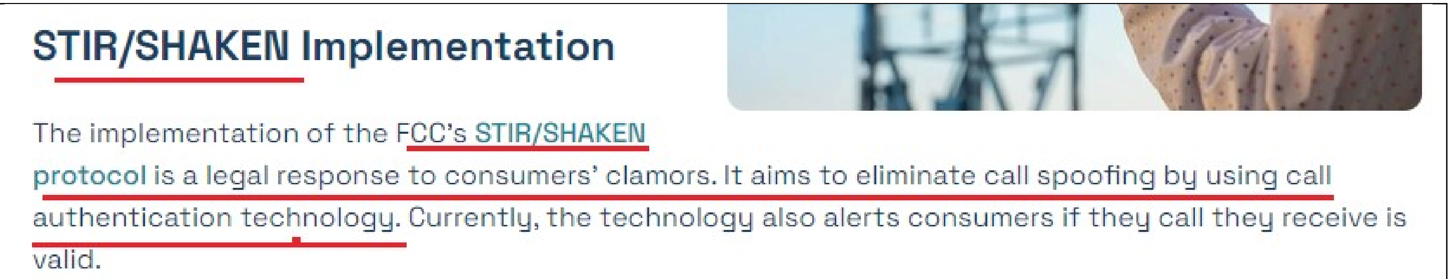
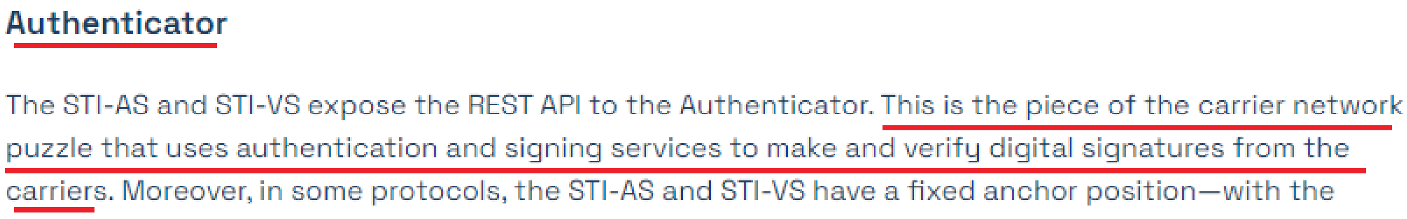
The SecureLogix® Call Secure™ Managed Service is powered by a team of call security experts with more than 400 years of collective experience. No team secures more enterprise voice networks, phone lines and calls than SecureLogix.

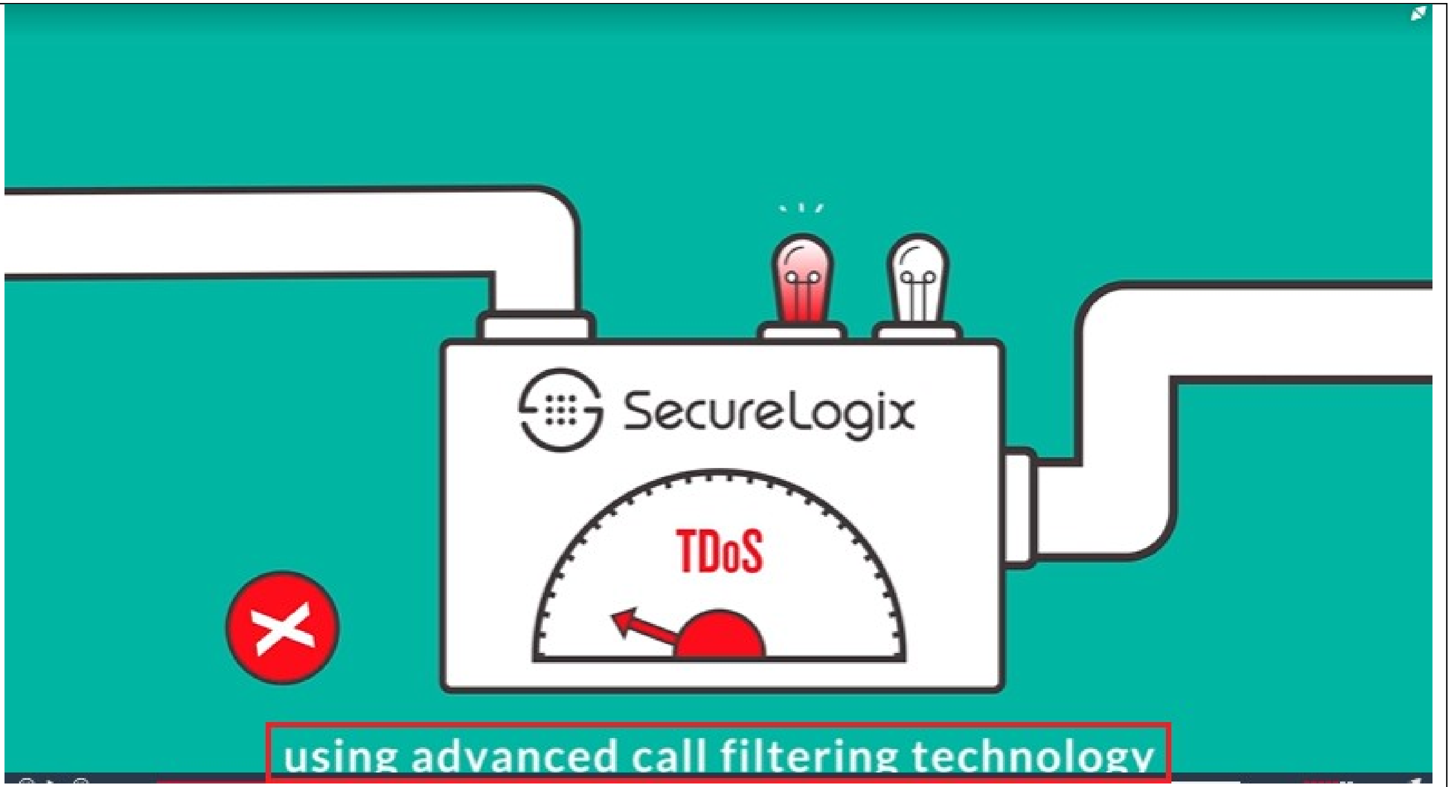
The Call Secure team also builds and maintains the Red List™ call threat database — a proprietary dataset of national harassing callers, voice spammers and call attack signatures. Red List is powered by the intelligence we gather from the enterprise voice attacks and malicious caller interactions that we see everyday. Every Call Secure customer benefits from Red List and it is a key ingredient in how we are able to continuously improve our ability to protect calls and network resources in a landscape where the threats are constantly changing and evolving.

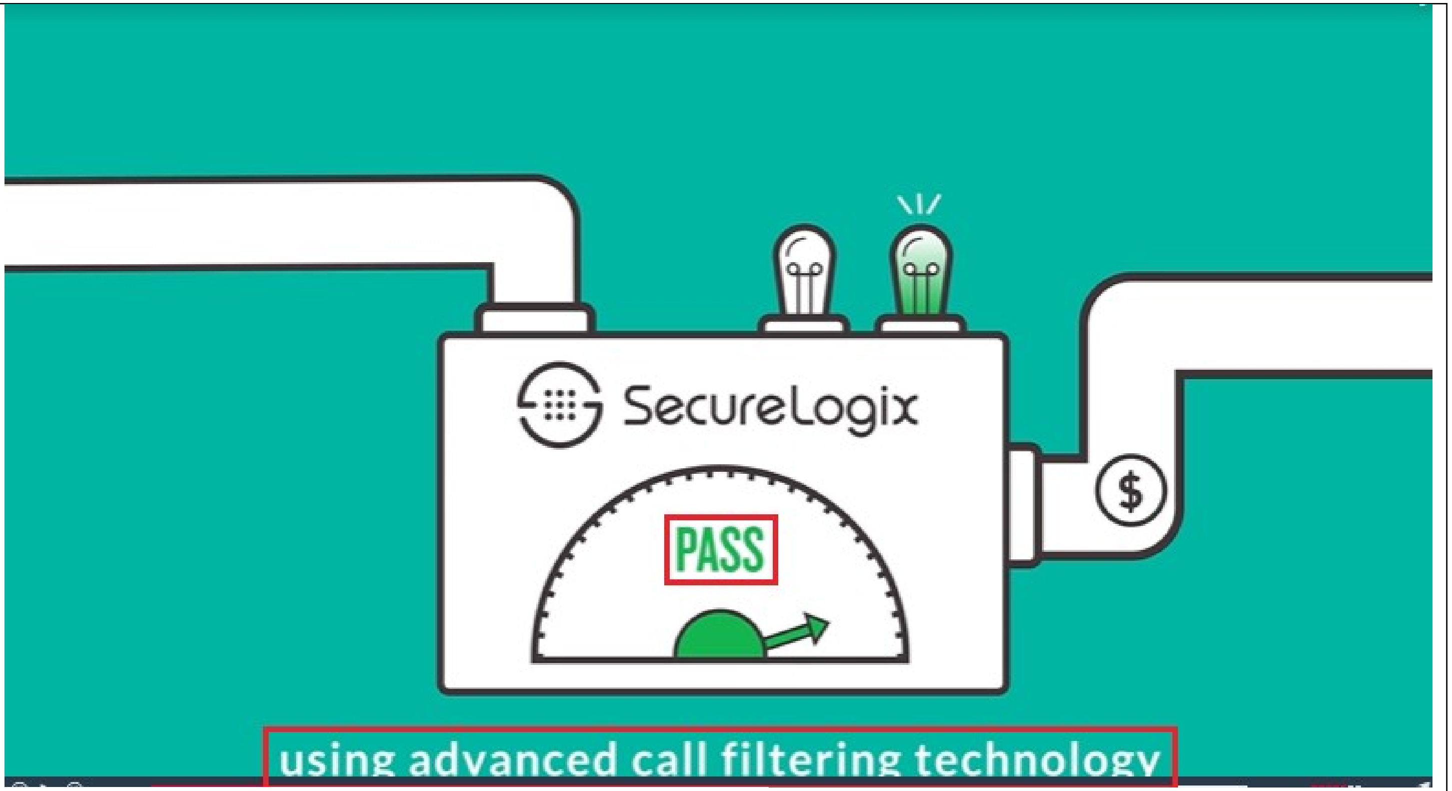
https://go.securelogix.com/downloads/flyers/call-secure

	 RED LIST™ caller profile database The Red List™ caller profile database is our proprietary database of harassing callers and attack signatures. A standard component of the Call Secure™ managed service solution, the Red List database is founded on 20 years of voice network protection experience. Red List leverages our broad and deep view of enterprise voice attacks and malicious caller interactions and we use this data to keep your voice network safe and secure day in and day out. **Caller Profiles** Red List is continuously updated with caller profile information helping us to identify and block nuisance callers. **Attack Signatures** We catalog known and emerging attack signatures so attacks can be quickly identified and defeated. https://securelogix.com/voice-network-security/

	 Governments and industry continue to work toward broad implementation of STIR/SHAKEN and its call attestation benefits. STIR/SHAKEN can indeed provide a substantial and credible means to help verify call identity. Even still, broad acceptance of STIR/SHAKEN alone will not solve all of the issues surrounding call identification, security and trust for the enterprise. Many gaps will remain, and enterprise and contact center environments will remain vulnerable to many types of robocalls and spoofed calling attacks. A broader architecture and set of technologies for call security and trust is required, along with an intelligent and efficient means to unify and optimize all of it. If properly orchestrated, this broader framework can powerfully lever STIR/SHAKEN across an ecosystem of other industry metadata sets, technology plugins, and industry fraud tools to deliver the most useful call identification results at the lowest cost. This approach extends STIR/SHAKEN to help complete the call verification and security puzzle in a highly affordable and scalable way for the enterprise. https://securelogix.com/events/stir-shaken-and-call-verification/

	 **STIR/SHAKEN Implementation** The implementation of the FCC's STIR/SHAKEN protocol is a legal response to consumers' clamors. It aims to eliminate call spoofing by using call authentication technology. Currently, the technology also alerts consumers if they call they receive is valid. https://calleridreputation.com/blog/understanding-how-shaken-tokens-work/  **Authenticator** The STI-AS and STI-VS expose the REST API to the Authenticator. This is the piece of the carrier network puzzle that uses authentication and signing services to make and verify digital signatures from the carriers. Moreover, in some protocols, the STI-AS and STI-VS have a fixed anchor position—with the https://calleridreputation.com/blog/understanding-how-shaken-tokens-work/

	 using advanced call filtering technology https://securelogix.com/voice-network-security/

	 SecureLogix PASS $ using advanced call filtering technology https://securelogix.com/voice-network-security/